In the Claims:

Please amend Claims 1, 7, 21, 26, 30 and 31, all as shown below. Applicant respectfully reserves the right to prosecute any originally presented or canceled claims in a continuing or future application.

1. (Currently amended) A system for maintaining security in a distributed computing environment, comprising:

(1) a policy manager, coupled to a network, including

a database for storing a security policy including a plurality of rules that control user access to applications; and

a policy distributor, coupled to the database, for distributing the plurality of rules through the network;

(2) a security engine located on a client coupled to the network and stored on a computer readable storage medium, said security engine ~~for~~ storing a set of the plurality of rules constituting a local customized security policy received through the network from the policy distributor, and ~~for~~ enforcing the local customized security policy with respect to an application at the client wherein enforcing the local customized security policy includes evaluating an access request by matching it to one or more of the plurality of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

(3) the application, coupled to the security engine, wherein the security engine guards access to the particular application to which said security engine is coupled, ~~such that~~ each separate application in the system ~~is~~ being guarded by a different copy of access authorization service such that separate applications in the system do not share authorization services ~~security engine~~; and

wherein the security policy is updated by recording a series of incremental changes to the security policy, determining which of said incremental changes are applicable to said security engine, computing an accumulated delta that reflects the series of incremental changes applicable to said security engine and sending the accumulated delta to the security engine from the policy manager such that the security engine uses the accumulated delta to update the local customized security policy.

2. (Previously presented) The system of claim 1, wherein the rules are stored separate from the application rather than being embedded in the application.

3. (Previously presented) The system of claim 1, wherein the security engine further comprises:

an engine for evaluating a request to access the application based on the set of the plurality of rules; and

an application programming interface (API) for enabling the application and the engine to communicate.

4. (Original) The system of claim 3, wherein the security engine further comprises: a plug-in application programming interface (API) for extending capabilities of the security engine.

5. (Original) The system of claim 1, further comprising: location means for enabling components in the system to locate each other through the network.

6. (Original) The system of claim 1, wherein the policy manager and the policy distributor are hosted on a first server, the security engine and the application are hosted on a second server, and the first and second servers are communicatively coupled to each other through the network.

7. (Currently amended) A system for maintaining security for an application in a distributed computing environment, comprising:

an engine located at a client coupled to a network and stored on a computer readable storage medium, the engine ~~for~~ storing a set of rules constituting a local customized policy received through the network from a centralized location, and ~~for~~ enforcing the local customized policy at an application level of the client;

an interface coupled to the engine for evaluating the local customized policy in order to control access to an application at the client wherein evaluating the local customized policy includes matching an access request to one or more of the plurality of rules of the local customized policy and granting or denying access to the application based on the evaluation; and

the application, coupled to the interface so as to communicate with the engine, wherein the engine guards access to the application that is coupled to said interface ~~such that~~ each separate application in the system ~~is~~ being guarded by a different copy of access authorization service such that separate applications in the system do not share authorization services ~~security engine~~;

wherein the local customized policy is updated by keeping track of incremental changes to the policy, determining which of said incremental changes are applicable to said engine, computing an accumulated delta that reflects all the incremental changes applicable to said engine and sending the accumulated delta to the engine from the centralized location such that the engine uses the delta to update the local customized policy.

8. (Previously presented) The system of claim 7, wherein the engine stores the rules separate from the application rather than being embedded in the application.

9. (Original) The system of claim 7, further comprising: a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

10-20. (Canceled)

21. (Currently amended) A method for maintaining security in a distributed computing environment, comprising:

maintaining a policy manager coupled to a network, including a database for storing a security policy and a policy distributor, coupled to the database, for distributing a portion of the security policy through the network;

maintaining a security engine located on a client coupled to the network, for storing a local customized security policy received through the network from the policy distributor, and for enforcing the local customized security policy with respect to an application at the client wherein enforcing the local customized security policy includes evaluating an access request by matching it to one or more of the plurality of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

maintaining the application, coupled to the security engine, wherein the security engine guards access to the particular application to which said security engine is coupled, ~~such that~~ each separate application in the system ~~is~~ being guarded by a different copy of access authorization service such that separate applications in the system do not share authorization services ~~security engine~~; and

receiving a series of incremental changes to the security policy at the policy manager;

determining which of said series of incremental changes are applicable to said security engine;

computing an accumulated delta that reflects the series of incremental changes that are applicable to said security engine; and

distributing the accumulated delta to the security engine on the client wherein the security engine uses the delta to update the local customized security policy.

22. (Previously presented) The method of claim 21, further comprising:

storing the accumulated delta in a policy change tracking table before distributing it to the security engine.

23. (Previously presented) The method of claim 22, further comprising:

reconstructing an updated local customized security policy back to a previously distributed version by using the accumulated delta stored in the policy change tracking table.

24. (Previously presented) The method of claim 21 wherein the security policy includes a plurality of rules for controlling access to securable objects.

25. (Previously presented) The method of claim 24 wherein the series of incremental changes include at least one or more of adding a rule, deleting a rule and amending a rule.

26. (Currently amended) A method for maintaining security in a distributed computing environment, comprising:

maintaining an engine at a client coupled to a network, the engine adapted to store a set of rules constituting a local customized policy received through the network from a centralized location, and for enforcing the local customized policy at an application level of the client;

maintaining an interface coupled to the engine for evaluating the local customized policy in order to control access to securable components wherein evaluating the local customized policy includes matching an access request to one or more of the set of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

maintaining the application, coupled to the interface so as to communicate with the engine, wherein the engine guards access to the application that is coupled to said interface ~~such that~~ each separate application ~~in the system is~~ being guarded by a different copy of access authorization service such that separate applications do not share authorization services ~~engine~~;

receiving a series of incremental changes to the set of rules at the centralized location;

determining which of said incremental changes are applicable to said engine;

computing an accumulated delta to reflect the series of incremental changes that are applicable to said engine; and

communicating the accumulated delta to the engine at the client such that the engine employs the accumulated delta to update the local customized policy.

27. (Previously presented) The method of claim 26, further comprising:

storing the accumulated delta in a policy change tracking table before distributing it to the engine.

28. (Previously presented) The method of claim 27, further comprising:

reconstructing an updated local customized policy back to a previously distributed version by employing the accumulated delta stored in the policy change tracking table.

29. (Previously presented) The method of claim 26 wherein the series of incremental changes include at least one or more of adding a rule, deleting a rule and amending a rule.

30. (Currently amended) A computer readable medium having instructions stored thereon which when executed by one or more processors cause a system to:

maintain a policy manager coupled to a network, including a database for storing a security policy and a policy distributor, coupled to the database, for distributing a portion of the security policy through the network;

maintain a security engine located on a client coupled to the network, for storing a local customized security policy received through the network from the policy distributor, and for enforcing the local customized security policy with respect to an application at the client wherein enforcing the local customized security policy includes evaluating an access request by matching it to one or more of the plurality of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

maintain the application, coupled to the security engine, wherein the security engine guards access to the particular application to which said security engine is coupled, ~~such that~~ each separate application ~~in the system is~~ being guarded by a different copy of access authorization service such that separate applications do not share authorization services ~~security engine~~; and

receive a series of incremental changes to the security policy at the policy manager;

determine which of said series of incremental changes are applicable to said security engine;

compute an accumulated delta that reflects the series of incremental changes applicable to said security engine; and

distribute the accumulated delta to the security engine on the client wherein the security engine uses the delta to update the local customized security policy.

31. (Currently amended) A computer readable medium having instructions stored thereon which when executed by one or more processors cause a system to:

maintain an engine at a client coupled to a network, the engine adapted to store a set of rules constituting a local customized policy received through the network from a centralized location, and for enforcing the local customized policy at an application level of the client;

maintain an interface coupled to the engine for evaluating the local customized policy in order to control access to securable components wherein evaluating the local customized policy includes matching an access request to one or more of the set of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

maintain the application, coupled to the interface so as to communicate with the engine, wherein the engine guards access to the application that is coupled to said interface ~~such that~~ each separate application ~~in the system is~~ being guarded by a different copy of access authorization service such that separate applications do not share authorization services ~~engine~~;

receive a series of incremental changes to the set of rules at the centralized location;

determine which of said series of incremental changes are applicable to said engine;

compute an accumulated delta to reflect the series of incremental changes applicable to said engine; and

communicate the accumulated delta to the engine at the client such that the engine employs the accumulated delta to update the local customized policy.